J. Symbolic Computation (1987) **4**, 351–364

A Generalization of Reduction Rings

SABINE STIFTER
Research Institute for Symbolic Computation
Johannes Kepler University
A-4040 Linz, Austria

(Received 15 May 1987)

In 1983 B. Buchberger introduced the notion of a reduction ring. Roughly, reduction rings are rings in which the Gröbner bases approach is possible. Reduction rings are characterized by axioms that relate the arithmetical operations in the ring with an ordering. In this paper we generalize this notion of a reduction ring by giving weaker axioms that characterize a wider class of rings. We also prove that the ring of integers modulo z, z an arbitrary not necessarily prime integer, is a reduction ring in this generalized sense.

1. Introduction

Buchberger (1983), (1983a) describes a generalization of the Gröbner bases algorithm introduced by Buchberger (1965), (1970). This generalization is different from all the other generalizations of the Gröbner basis approach that have been considered in the literature. The crucial difference is that in Buchberger's approach "first order" axioms for the arithmetical operations of a ring and an additional ordering relation are formulated such that

> if a ring satisfies these axioms (is a "reduction ring")
> then the notion of a Gröbner basis can be formulated in the ring
> and Buchberger's algorithm can be used for constructing Gröbner bases.

The axioms are "first order" in the sense that their formulation does not involve sets of elements in the ring but, similar to the usual axioms of algebraic nature like associativity, commutativity etc., involves only ring elements, operations on elements and the additional order predicate. In particular, no "grading" (for example, polynomial structure) is necessary in the ring as it is the case, for example, in the approach of Robbiano (1986). Also, in Buchberger's approach it is not necessary to presuppose algorithmic solvability of "higher order" problems (like the membership problem or the problem of computing syzygies) in the coefficient domain

0747–7171/87/060351+14 $03.00/0

in order to compute Gröbner bases in the polynomial ring over the coefficient domain. Such "higher order" assumptions are necessary in other approaches, for example, in Schaller (1979), Trinks (1978), Zacharias (1978).

Once a ring R is shown to be a reduction ring one can compute Gröbner bases in the polynomial ring over this ring R as coefficient domain. However, one can also compute Gröbner bases in the ring R itself. This is not possible in the approaches of Schaller (1979), Trinks (1978), Zacharias (1978). Buchberger's (1983) approach does not really extend the class of rings that are known to admit a Gröbner bases construction. The emphasis is on the new methodology that is different from the other approaches. Actually, Z_z is the only example of a ring known to be amenable to Buchberger's approach without an apparent Gröbner bases construction in the other approaches. We give the details of this example in this paper.

The absence of any additional structure on reduction rings makes it necessary to introduce a totally new approach for the formulation of critical pairs that involves only the arithmetical operations and the order predicate. This is done by defining a natural reduction relation based on the arithmetical operations and the order predicate and the new concept of a "least common reducible" of two elements based on the reduction relation. The "least common reducible" is a very general concept whose formulation seems to be possible whenever a "reduction relation" is available in a structure and, hence, might yield an interesting approach to the critical pair technique in much more general structures than just rings. This research direction has not yet been pursued.

Very little structure is presupposed in Buchberger's approach. As a consequence, the construction that build up critical pairs and Gröbner bases from the ring operations, though conceptionally simple, are quite involved technically. In this paper, we go even one step further. We show that the axiomatic assumptions can be made even weaker. As a practical consequence, more rings satisfy the axioms and, hence, are amenable to the reduction ring approach.

In particular, although in principle the reduction ring axioms allow the ring R to have zero divisors, no ring with zero divisors has been proved to be a reduction ring. (The proof by Rolletschek (1983) that Z_z, i.e. the ring of integers modulo z, z an arbitrary not necessarily prime integer, is a reduction ring is not correct: in proof of axiom (A4) the case $b_1 = b_2$ is not considered; compare the following example.)

Consider Z_8, together with the order relation $<'$ and the set of multipliers M as defined by Rolletschek (1983), i.e. $0 <' 1 <' \cdots <' 7, M =$

$\{1,3,5,7\}$. Let $a = 6$, $c = 4$, $m_1 = 1$, $m_2 = 3$. Then

$$2 = 6 - 1 * 4 \leftarrow_4 6 \rightarrow_4 6 - 3 * 4 = 2.$$

In a reduction ring (by axiom (A4), see Buchberger (1983)) in such a situation it must be possible to find $l_1, \ldots, l_k$, $k \geq 0$, such that

(1) $\quad l_1, \ldots, l_k \in M,$

(2) $\quad a - m_1 c \leftrightarrow_c a - m_1 c - l_1 c \leftrightarrow_c \cdots a - m_1 c - l_1 c - \cdots - l_k c =$
$\quad = a - m_2 c,$

(3) $\quad a - m_1 c - l_1 c - \cdots - l_j c <' a, \quad$ for $0 \leq j \leq k, \quad$ and

(4) $\quad m_1 + l_1 + \cdots + l_k = m_2.$

By (4) and $m_1 \neq m_2$ it follows $k > 0$. So there must exist $l_1 \in M$ such that $a - m_1 c - l_1 c <' a$ (by (1) and (3)), i.e. there exists j, $0 \leq j < z/2$ such that

$$a - m_1 c - (2j+1)c <' a, \quad \text{i.e.} \quad 6 <' 6$$

in contradiction to the definition of $<'$. (If l_1 is not of the form $2j+1$ then l_1 is a zero divisor and therefore not in M.)

From this example one sees that one has to overcome two difficulties: Firstly, in a ring with zero divisors, there may exist sets F with only one element that are not Gröbner bases. (In reduction rings in the sense of Buchberger (1983) sets with only one element are always Gröbner bases.) Secondly, the set of multipliers M is too large. There are situations in which an element can be reduced using two different reductions, involving two different multipliers, both giving the same result. However, making the set of multipliers M smaller to avoid such ambiguous situations would contradict other axioms of a reduction ring.

Our main idea is to allow for each element c of R a distinct set of multipliers $M_c \subset R$ instead of only one set of multipliers M for all elements c of R. Secondly, the definition of critical pairs is restricted. As a consequence, zero divisors may also be allowed in the set of multipliers M_c. This is one of the reasons why Z_z can be proved to be a reduction ring in our sense (see below). A second consequence is that a set $F \subset R$ with only one element need not be a Gröbner basis any more. This yields another degree of freedom.

Correspondingly the definition of critical pairs and the axioms defining a reduction ring have to be modified in a way such that the correctness

of the Gröbner bases algorithm can still be proved and the property of being a reduction ring carries over from R to $R[x_1, \ldots, x_n]$, as it is done by Buchberger (1983).

The axioms for a reduction ring given below are weaker than the axioms given by Buchberger (1983). Every ring R together with the order relation $<$ on R and the set of multipliers M that satisfies the axioms of a reduction ring in the sense of Buchberger (1983) also satisfies the new axioms for a reduction ring where $M_c := M$ for each $c \in R$. Furthermore, there are examples of rings satisfying our new axioms that are not reduction rings in the sense of Buchberger (1983).

2. Reduction and Critical Pairs

Let R be a commutative ring with 1 (possibly with zero divisors), $<$ a noetherian partial order relation and M_c, M_c^+, $M_c^- \subset R$ for each $c \in R$. For each $c \in R$ let M_c^+ and M_c^- be such that $M_c^+ \cup M_c^- = M_c$. (One of the two subsets may possibly be empty.)

Some typed variables will be used:

a, b, c, d, e	for elements of R,
l, m, n	for elements of M_c,
C, D	for subsets of R,
i, j, k	for elements of N, (natural numbers),
f, p, q, r	for elements of $R[x_1, ..., x_n]$,
s, t, u	for n-variate power products.

By Ideal(F) we denote the ideal generated by F.

The following definitions are taken from Buchberger (1983). The definition of a common reducible and the definition of a critical pair, however, needs some modification by introducing the concept of *irrelative* multiples. Both definitions use two different sets of multipliers M_c^+ and M_c^- for each $c \in R$.

Definition :

$$a \rightarrow_{(m,c)} b \quad \text{iff} \quad b = a - mc,\ m \in M_c,\ b < a.$$

(a is *reducible* to b modulo c by m)

$$a \rightarrow_c b \quad \text{iff} \quad (\exists m)(a \rightarrow_{(m,c)} b).$$

$a \to_c$ iff $(\exists b)(a \to_c b)$.

$a \to_C$ iff $(\exists c \in C)(a \to_c)$

$a \downarrow_c^* b$ iff $(\exists d)(a \to_c^* d \text{ and } b \to_c^* d)$.
(a and b have a *common successor* modulo c)

(*Remark* : We write $\to$ instead of $\to_c$ if it is clear from the context what c is.)

$\leftrightarrow$, $\to^*$, $\leftrightarrow^*$ are the symmetric, the reflexive transitive and the reflexive transitive symmetric closure of a reduction relation $\to$, respectively.

a is in *normal form w.r.t.* C
iff not $a \to_C$.

a is *a normal form of* b *w.r.t.* C
iff $b \to_C^*$ and
a is in normal form w.r.t.C.

$a \leftrightarrow^* (< d) b$ iff $(\exists e_0, \ldots, e_n)$
$(a = e_0 \leftrightarrow e_1 \leftrightarrow \cdots \leftrightarrow e_n = b$
and $e_0, \ldots, e_n < d)$.
(a and b *can be connected below* d)

(m_1, c_1) and (m_2, c_2) are *irrelative*
iff $(c_1 \neq c_2)$ or
$(c_1 = c_2, m_1 \in M_{c_1}^+, m_2 \in M_{c_1}^-)$ or
$(c_1 = c_2, m_2 \in M_{c_1}^+, m_1 \in M_{c_1}^-)$.

a is a *common reducible* for c_1 and c_2
iff $(\exists m_1, m_2)$
$(a \to_{(m_1,c_1)}, a \to_{(m_2,c_2)}$ and
$(m_1, c_1), (m_2, c_2)$ irrelative).

$c_1 \triangle^a c_2$ iff a is a common reducible for c_1 and c_2,
not $(\exists m_1, m_2)$
$(a - m_1 c_1 \leftarrow_{(m_1,c_1)} a \to_{(m_2,c_2)} a - m_2 c_2$,
$a - m_1 c_1 \to_{(m_2,c_2)} a - m_1 c_1 - m_2 c_2$ or

$$a - m_2c_2 \rightarrow_{(m_1,c_1)} a - m_2c_2 - m_1c_1,$$
$$(m_1, c_1) \text{ and } (m_2, c_2) \text{ irrelative}).$$

(a is a *non-trivial common reducible* for c_1 and c_2)

$c_1 \underline{\triangle}^a c_2$ iff $c_1 \triangle^a c_2$,
$(\forall a' : a' < a)(\neg c_1 \triangle^{a'} c_2)$.

(a is a *minimal non-trivial common reducible* for c_1 and c_2)

$c\triangle^a$ iff $a \rightarrow_c$,
not $(\exists m_1, m_2)$
$(a - m_1c \leftarrow a \rightarrow a - m_2c \rightarrow a - m_2c - m_1c)$.

(a is a *non-trivial reducible for* c)

$c\underline{\triangle}^a$ iff $c\triangle^a$,
not $(\exists a' : a' < a)(c\triangle^{a'})$.

(a is a *minimal non-trivial reducible for* c)

b_1, b_2 *constitute a critical pair* for c_1 and c_2 w.r.t. a
iff $c_1 \underline{\triangle}^a c_2$,
$(\exists m_1, m_2)(a \rightarrow_{(m_1,c_1)} a - m_1c_1 = b_1$,
$a \rightarrow_{(m_2,c_2)} a - m_2c_2 = b_2$,
(m_1, c_1) and (m_2, c_2) irrelative).

Note that there is a difference between $c\triangle^a c$ and $c\triangle^a$. This difference is crucial. More precisely: $c\triangle^a c$ does not imply $c\triangle^a$ because there can exist m_1, m_2 such that (m_1, c) and (m_2, c) are not irrelative and $a - m_1c \leftarrow a \rightarrow a - m_2c \rightarrow a - m_2c - m_1c$. On the other hand $c\triangle^a$ does not imply $c\triangle^a c$ because not necessarily there exists m_1, m_2 such that $(m_1, c), (m_2, c)$ irrelative and $a - m_1c \leftarrow a \rightarrow a - m_2c$.

The meaning of $\equiv$ is as usual:

$$a \equiv_C b \quad \text{iff} \quad a = b + \sum_{1 \le i \le k} d_i c_i \quad \text{for some} \quad k, d_i \in R, c_i \in C.$$

As one will see after the definition of a reduction ring the splitting of M_c in the definitions above provides an additional degree of freedom for the set of multipliers. However, this splitting of the M_c will only influence the construction of critical pairs for two elements c_1 and c_2, where $c_1 = c_2$ and, hence, the construction of a Gröbner basis (see below). Once a Gröbner

basis has been calculated one need not take care of the chosen splitting any longer.

3. Reduction Rings

Definition :

Let R be a commutative ring with 1, $<$ a noetherian partial order relation on R, M_c, M_c^+, $M_c^- \subset R$ for each $c \in R$.

R together with $<$ and M_c, M_c^+, M_c^- constitute a reduction ring iff $M_c^+ \cup M_c^- = M_c$ for each c, and the following axioms are satisfied:

(R0) $1 \in M_c$ for each $c \in R, c \neq 0$.

(R1) If $m \in M_c$ then $-m \in M_c$.

(R2) If $m \in M_c$, $c \neq 0$ then $mc \neq 0$.

(R3) $(\exists m_1, \ldots, m_n \in M_c)(b = \sum_{1 \leq i \leq n} m_i)$ for each $b, c \neq 0$.

(R4) If $a \neq 0$ then $a > 0$.

(R5) If $a \rightarrow_{(m',c)} b$
then $(\forall d)(\exists m_1, \ldots, m_x, n_1, \ldots, n_y)$
$(a + d \rightarrow_{(m_1,c)} a + d - m_1 c \rightarrow \cdots$
$\rightarrow_{(m_x,c)} a + d - m_1 c - \cdots - m_x c =$
$= b + d - n_1 c - \cdots - n_y c \leftarrow \cdots$
$\leftarrow b + d - n_1 c \leftarrow_{(n_1,c)} b + d,$
$m_1 + \cdots + m_x = m' + n_1 + \cdots + n_y)$.

(R6) If $a - m_1 c \leftarrow_{(m_1,c)} a \rightarrow_{(m_2,c)} a - m_2 c$, $(m_1, c), (m_2, c)$ not irrelative (i.e. $m_1, m_2 \in M_c^+$ or $m_1, m_2 \in M_c^-$)
then $(\exists l_1, \ldots, l_k)$
$(a \rightarrow_{(m_1,c)} a - m_1 c \leftrightarrow_{(l_1,c)} a - m_1 c - l_1 c \leftrightarrow \cdots$
$\leftrightarrow_{(l_k,c)} a - m_1 c - \cdots - l_k c = a - m_2 c,$
$a - m_1 c - l_1 c - \cdots - l_j c < a, 1 \leq j \leq k,$
$l_1 + \cdots + l_k + m_1 = m_2)$.

(R7) If $c_1 \triangle^a c_2$
then $(\exists a' : a' \leq a)(\exists m)$
(1) $c_1 \triangle^{a'} c_2$,
(2) $m' \in M_c \Rightarrow mm' \in M_c$, for all m', c,

(3) $a' > a' + c \quad \Rightarrow \quad a > a + mc$, for all c,
(4) $b \rightarrow_c d \quad \Rightarrow \quad mb \leftrightarrow_c md$, for all b, c, d,
(5) $(a' \rightarrow_{(m_1,c_1)}, a' \rightarrow_{(m_2,c_2)},$
$(m_1, c_1), (m_2, c_2)$ irrelative)
$\Rightarrow \quad ((mm_1, c_1), (mm_2, c_2)$ irrelative),
for all m_1, m_2.

(R8) If $c\triangle^a$
then $(\exists a' : a' \leq a)(\exists m)$
(1) $c\triangle^{a'}$,
(2) $m' \in M_{c'} \quad \Rightarrow \quad mm' \in M_{c'}$, for all m', c,
(3) $a' > a' + c \quad \Rightarrow \quad a > a + mc'$, for all c',
(4) $b \rightarrow_{c'} d \quad \Rightarrow \quad mb \leftrightarrow_{c'} md$, for all b, c', d.

(RT1) There exists no infinite sequence $D_1, D_2, \ldots$ of subsets of R such that $Red(D_1) \subset Red(D_2) \subset \ldots$, where $\subset$ is strict set inclusion, $Red(D) := \{a | a \rightarrow_D\}$.
(RT2) For all c_1, c_2, c the sets $\{a | c_1 \underline{\triangle}^a c_2\}$ and $\{a | c \underline{\triangle}^a\}$ are finite.
(RE1) $<$ is decidable on R.
(RE2) There exists an algorithm A such that for all a, c
$(\exists m \in M_c^+)(a \rightarrow_{(m,c)}) \quad \Rightarrow \quad a - A(a,c)c < a, A(a,c) \in M_c^+$ and
$(\exists m \in M_c^-)(a \rightarrow_{(m,c)}) \quad \Rightarrow \quad a - A(a,c)c < a, A(a,c) \in M_c^-$.

Some remarks about the axioms:

Most of the axioms are carried over from Buchberger (1983) with only slight modifications implied by using different sets of multipliers M_c instead of M.

The axioms (M3) and (A3) of Buchberger (1983) appear in (R7) and (R8) in a weaker form.

Because of the separate sets of multipliers M_c for each c and the fact that (M3) is only needed for some very special m, the axiom (M4) of Buchberger (1983) can be replaced by a much weaker axiom (R2).

The axiom (R3) is the analogue of axiom (M5') of Buchberger (1983), the axiom (M5) cannot be transformed directly.

Theorem :

Let R be a commutative ring with 1, $<$ a noetherian order relation on R, $M \subseteq R$ such that R together with $<$ and M constitutes a reduction

ring in the sense of Buchberger (1983). Then R together with $<$ and $M_c^+ := M_c^- := M_c := M$ for each c constitute a reduction ring (in the sense of this paper).

Proof :

In this special case the definitions for a common reducible as well as the definitions for a critical pair in the sense of Buchberger (1983) and in the sense of this paper, respectively, are the same. Hence we only have to show that the axioms of Buchberger (1983) imply the axioms of this paper. The proof of this implication is straightforward.

Lemma :

$a \leftrightarrow_C^* \quad \Leftrightarrow \quad a \equiv_C b.$

The proof of this lemma can be carried over from Buchberger (1983) without change.

4. Gröbner Bases

The definition of the Church-Rosser property is standard, the definition of Gröbner bases is taken from Buchberger (1983).

Definition :

$\rightarrow$ has the *Church-Rosser property* iff for all a, b : If $a \leftrightarrow^* b$ then $a \downarrow^* b$.

$D \subset R$ is a *Gröbner basis* iff $\rightarrow_D$ has the Church- Rosser property.

$D \subset R$ is a *reduced Gröbner basis* iff D is a Gröbner basis and for each $d \in D$: d is in normal form w.r.t. $D - \{d\}$.

Presupposition :

From now on presuppose that R, $<$, M_c, M_c^+, M_c^- for each $c \in R$ constitute a reduction ring.

We now state the main theorem for the new notion of reduction rings. This theorem shows that in reduction rings Gröbner bases can be constructed by Buchberger's algorithm.

Main theorem for constructing Gröbner bases:

C is a Gröbner basis iff

for all $c_1, c_2 \in C$ and a such that $c_1 \overline{\triangle}^a c_2$ there exists a critical pair b_1, b_2 for c_1, c_2 w.r.t. a such that $b_1 \leftrightarrow^* (< a) b_2$.

The proof of this theorem can be modeled after the proof by Buchberger (1983), (1983a). It is based on the generalized Newman-Lemma introduced by Buchberger (1983), whose proof is included in Winkler, Buchberger (1983). The details of the proof of this theorem using the definitions of this paper are contained in Stifter (1985).

Problem of constructing Gröbner bases:

Given:

A finite set $C \subseteq R$.

Find:

A finite set $D \subseteq R$ such that
$\leftrightarrow_C^* \;=\; \leftrightarrow_D^*$ and
$\rightarrow_D$ has the Church-Rosser property.

Buchberger's algorithm for constructing Gröbner bases:

$D := C$
$B := \{(\{c_1, c_2\}, a) |\quad c_1, c_2 \in C, \quad c_1 \underline{\triangle}^a c_2\}$
<u>while</u> $B \neq \emptyset$ <u>do</u>
$(\{c_1, c_2\}, a) \;:=$ a pair out of B
$B \;:= B - \{(\{c_1, c_2\}, a)\}$
$(b_1, b_2) \;:=$ two elements such that $b_1 \leftarrow_{c_1} a \rightarrow_{c_2} b_2$
$(b_1, b_2) \;:=$ (normal form of b_1, normal form of b_2) (w.r.t. D)
<u>if</u> $b_1 \neq b_2$ <u>then</u>
$c := \; b_1 - b_2$
$B := \; B \cup \{(\{c, c'\}, a) | c' \in D, c \underline{\triangle}^a c'\} \cup \{(\{c, c\}, a) | c \underline{\triangle}^a c\}$
$D := \; D \cup \{c\}$

The algorithm is identical to the algorithm given by Buchberger (1983). Note, however, that in the line before the last line of the algorithm, where B is updated, also all pairs $(\{c, c\}, a)$ are added to B, where a is a minimal non-trivial reducible for c and c. This ensures, that also critical pairs for one element c in the basis are considered. For a proof of the partial correctness and the termination of the algorithm see Buchberger (1983). The proof given there can be carried over without any changes using the definitions and the main theorem given above.

5. Polynomial Reduction Rings

The property of being a reduction ring still carries over from a ring R to $R[x_1, \ldots, x_n]$, the ring of polynomials in n variables over R, as it is the case for reduction rings in the sense of Buchberger (1983). Before we give

the theorem how to define the order relation on the polynomials and the set of multipliers for the polynomials, we need one more definition.

Definition: (Trinks (1978), Buchberger (1983))

Let $\prec$ be an order relation on power products. $\prec$ is called admissible iff
(PP1) $(\forall s \neq 1)(1 \prec s)$ and
(PP2) $(\forall s,t,u)(s \prec t \quad \Rightarrow \quad su \prec tu)$.

From (PP1) and (PP2) one gets immediately
(PP3) $(\forall s,t)(s \text{ divides } t, s \neq t \quad \Rightarrow \quad s \prec t)$.

The following notation will be used: $C(p,t)$, $H(p,t)$, $L(p,t)$, $LC(p)$, $LP(p)$, $LM(p)$, and $R(p,t)$ denote the coefficient of p at t, the higher part and the lower part of p w.r.t. t, the leading coefficient, the leading power product and the leading monomial of p, and the rest of p w.r.t. t, respectively.

Theorem for polynomial reduction rings

Let R together with $<$ and M_c for each c be a reduction ring. Then $R[x_1,\ldots,x_n]$ together with $\ll$ and MP_f, MP_f^+, MP_f^- for each f constitutes a reduction ring, where

$MP_f^+ := \{ms \mid \quad m \in M_c^+, c = LC(f), s \text{ an n-variate power product}\}$,
$MP_f^- := \{ms \mid \quad m \in M_c^-, c = LC(f), s \text{ an n-variate power product}\}$,
$MP_f := MP_f^+ \cup MP_f^-$,
$p \ll q :\Leftrightarrow (\exists t)(H(p,t) = H(q,t), C(p,t) < C(q,t))$.

The proof of this theorem can again be modeled after the proof of the corresponding theorem of Buchberger (1983), (1983a). The details of the proof using the definitions of this paper can be found in Stifter (1985). In the following we only sketch the main differences to the proof of Buchberger (1983a). For the proof the fact that still

$$LP(muf) = uLP(f), \text{ if } mu \in MP_f,$$

is crucial. The property (RED) of Buchberger (1983a) is reformulated to

$$p \rightarrow_{(mu,f)} p - muf \quad \text{iff} \quad C(p,t) \rightarrow_{(m,LC(f))} C(p,t) - mLC(f),$$

where $t = uLP(f)$, to distinguish the different sets of multipliers for each element. We also had to reformulate the properties (CR1) and (CR2) of Buchberger (1983) to distinguish the two kinds of non-trivial reducibles. The formulation of (CR1) and (CR2) of Buchberger (1983a) will not work for the definitions of this paper. The reformulated properties are:

(CR1) $f_1 \triangle^p f_2$ iff not $(\exists t_1, t_2 : t_1 \neq t_2)$
$(LP(f_1)$ divides $t_1, C(p,t_1) \rightarrow_{LC(f_1)}$,
$(LP(f_2)$ divides $t_2, C(p,t_2) \rightarrow_{LC(f_2)}$ and
$(\exists t)(LP(f_1)$ divides $t, LP(f_2)$ divides t,
$LC(f_1) \triangle^{C(p,t)} LC(f_2)$
if $(f_1 = f_2$ or $LC(f_1) \neq LC(f_2))$
and $LC(f_1) \triangle^{C(p,t)}$ otherwise).

$f \triangle^p$ iff not $(\exists t_1, t_2 : t_1 \neq t_2)$
$(LP(f)$ divides $t_1, C(p,t_1) \rightarrow_{LC(f)}$,
$(LP(f)$ divides $t_2, C(p,t_2) \rightarrow_{LC(f)}$ and
$(\exists t)(LP(f)$ divides t, $LC(f) \triangle^{C(p,t)})$.

(CR2) $f_1 \underline{\triangle}^p f_2$ iff $p = LC(p) LCM(LP(f_1), LP(f_2))$,
$LC(f_1) \underline{\triangle}^{LC(p)} LC(f_2)$
if $(f_1 = f_2$ or $LC(f_1) \neq LC(f_2))$
and $LC(f_1) \underline{\triangle}^{LC(p)}$ otherwise.

$f \underline{\triangle}^p$ iff $p = LC(p) LP(f)$, $LC(f) \underline{\triangle}^{LC(f)}$.

6. Example $Z_z, z \in N$

We show that Z_z, i.e. the residue class ring of the integers modulo z, is a reduction ring, where z is an arbitrary not necessarily prime integer. This is the first time that the Gröbner bases approach can be applied to a ring with zero divisors.

Definition:

As a representation of Z_z we take $Z_z = \{0, 1, \ldots, z-1\}$, ordered by

$$0 <' 1 <' \cdots <' z-1.$$

$M_c^+ := \{m |\ 0 <' m <' n, n$ the least element of Z_z not equal to 0, such that $nc = 0\}$, $M_c^- := \{m |\ -m \in M_c^+\}$, $M_c := M_c^+ \cup M_c^-$.

Theorem:

$Z_z, <', M_c^+, M_c^-$ for each c constitute a reduction ring.

Proof:

$<'$ is a noetherian order relation on Z_z because $<$ is noetherian on Z.

Proof of the axioms of a reduction ring:

(R0): Let $c \in Z_z, c \neq 0$. Then $1c \neq 0$, therefore $1 \in M_c$.

(R1): Let $m \in M_c$. Then $-m \in M_c$ by definition of M_c.

(R2): Let $m \in M_c$. Then $m <' n$ or $-m <' n$, where n is the least element of Z_z not equal to 0 (w.r.t. $<'$) such that $nc = 0$. Therefore $mc \neq 0$.

(R3): Let $b, c \in Z_z, b \neq 0, c \neq 0, m_i := 1, n := b$. Then $m_i \in M_c$ by (R0), $\sum_i m_i = n1 = b$.

(R4): If $a \neq 0$ then $a >' 0$, trivially.

(R5): Let $a \rightarrow_{(m,c)} b, d$ arbitrary. Because $<'$ is a total order relation one of the following cases must hold: $a + d >' b + d$ or $a + d <' b + d$. ($a + d = b + d$ is not possible because in this case $a = b$.) Therefore $a + d \rightarrow_{(m,c)} b + d$ or $a + d \leftarrow_{(-m,c)} b + d$.

(R6): Let $a - m_1 c \leftarrow_{(m_1,c)} a \rightarrow_{(m_2,c)} a - m_2 c$, $(m_1, c), (m_2, c)$ irrelative.
Case: $m_1, m_2 \in M_c^+$.
Subcase $m_1 = m_2$: trivial.
Subcase $m_1 >' m_2$: In this case $m_1 - m_2 <' m_1$ and hence $(m_1 - m_2) \in M_c$. Therefore $a - m_1 c \leftrightarrow_{(m_1 - m_2, c)} a - m_2 c$.
Subcase $m_1 <' m_2$: Analogous to the subcase above.
Case: $m_1, m_2 \in M_c^-$.
Analogous to the case above.

(R7): Assume $c_1 \triangle^a c_2$. Trivially there exists an a', $a' \leq' a$, $c_1 \underline{\triangle}^{a'} c_2$, $m := 1$. (1) holds by choice of a'. By the fact (see Rolletschek (1983)) that $a' + c <' a'$ iff $a' + c \geq z$ and $a + c \geq a' + c$ one gets $a + c \geq z$ and hence $a + c <' a$. Because of $m = 1$ (2), (4) and (5) are satisfied trivially.

(R8): Assume $c \triangle^a$. Then there exists a' such that $a' \leq' a$, $c \underline{\triangle}^{a'}$, $m := 1$. (1) holds by choice of a', (3) follows exactly as in the proof of (R7). (2) and (4) hold trivially because $m = 1$.

(RT1), (RT2), (RE1) and (RE2) hold because Z_z is finite.

For practical purposes it will be necessary to have easy formulae for the least common reducible of two elements c_1 and c_2 and an easy algorithm $A(a, c)$ for computing multipliers.

Let $LR(a)$ denote the least reducible of a, $LCR(a, b)$ denote the least common reducible of a and b.

If $a = LR(c)$ then $a = mc$ for some $m \in M_c$. It is a well known fact that $a = mc$ is solvable for an $m \in Z_z$ iff $a = kGCD(c, z)$, for some k. The least multiple of $GCD(c, z)$ is in the given order relation $<'$ the $GCD(c, z)$ itself. Furthermore, if $a \rightarrow_c$ and $a' >' a$ then $a' \rightarrow_c$. So we get

$$LCR(a, b) = max_{<'}\{LR(a), LR(b)\}, \quad A(a, c) := a/c,$$

where $LR(a) = GCD(a, z)$. ($GCD(a, b)$ denotes the greatest common divisor af a and b, / denotes division in Z_z.)

References

Buchberger, B. (1965). An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal (German). Univ. of Innsbruck, Math. Inst., Ph. D. thesis.

Buchberger, B. (1970). An algorithmical criterion for the solvability of algebraic systems of equations (German). *Aequationes mathematicae* 4 (3), 374–383.

Buchberger, B. (1983). A critical-pair/completion algorithm in reduction rings. *Proceedings Logic and Machines: Decision Problems and Complexity*, (eds. E. Börger, G. Hasenjäger, D. Rödding), *Springer Lect. Notes Comp. Sci.* **171**, 137–161.

Buchberger, B. (1983a). A critical-pair/completion algorithm in reduction rings. Univ. of Linz, Math. Inst., Technical report no. CAMP-83-21.0.

Robbiano, L. (1986). On the theory of graded structures. *Journ. of Symbolic Computation*, **2** (2), Academic Press, (ed. B. Buchberger), 139–170.

Rolletschek, H. (1983). Proof that Z_z is a reduction ring. Univ. of Linz, Math. Inst., contained as part of Technical report no. CAMP-83-21.0, also in Buchberger (1983).

Schaller, S. (1979). Algorithmic aspects of polynomial residue class rings. Univ. of Wisconsin-Madison, Comp. Scie. Dept., Ph. D. thesis, Technical report no. 370.

Stifter, S. (1985). Gröbner bases over the integers and in general reduction rings. Univ. of Linz, Math. Inst., Diploma thesis, Technical report no. CAMP-85-28.0.

Trinks, W. (1978). On B. Buchberger's method for solving systems of algebraic equations (German). *Journ. Number Theory*, 10 (4), 475–488, (preprint 1977).

Winkler, F., Buchberger, B. (1983). A criterion for eliminating unnecessary reductions in the Knuth-Bendix algorithm. *Proceedings of the Coll. on Algebra, Combinatorics and Logic in Comp. Sci.*, Györ, Coll. Math. Soc. J. Bolyai, North Holland.

Zacharias, G. (1978). Generalized Gröbner bases in commutative polynomial rings. Bachelor thesis, M.I.T., Comp. Scie. Dept.